Оптимизация затрат на мероприятия по киберзащите РЗА

RTSoft
средства и системы автоматизации

Павел Литвинов

RUGRIDS ELECTRO

декабрь, 2016

VI Международная научно-практическая конференция
“АВТОМАТИЗАЦИЯ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭНЕРГЕТИКЕ 2016

Принципы планирования защиты

- Адекватность существующей (текущей) модели угроз – экономическая целесообразность
- Архитектурно заложенный «запас прочности» под будущие угрозы – защита инвестиций
- Переоценка роли эффективности дублирования (многократного резервирования) и его влияния на надежность в случае кибератак
- «Эшелонированность обороны», отступление на заранее подготовленные позиции: заранее определенная деградация части функций
- Распределенность защитных мер и их ассиметричная реализация
- Правильный учет «человеческого фактора»

- **Готовность к «техническому регрессу» ради безопасности**

Оптимизационная задача – сложная функция от:

- Начальных (граничных) условий
  - масштаб организации (задачи)
  - наличие требований регуляторов
- Точки зрения
  - специалист по ИБ
  - руководитель
  - собственник
- Стратегии (сценарии)
  - «модернизация»
  - «новое строительство»

Идея:
минимизация каждого множителя:

- **Угроза – не нападают**
- **Уязвимость – нет уязвимостей**
- **Последствие – мин. последствия**

Уменьшает РИСК

УГРОЗА	x	УЯЗВИМОСТЬ	x	ПОСЛЕДСТВИЕ	=	РИСК
Событие, действующее лицо или действие, которое потенциально может нанести вред		Недостаток		Воздействие		На операции, экономику, безопасность, окружающую среду
Какие угрозы нас беспокоят?		Оценить воздействие уязвимых мест в киберпространстве.		Каково физическое воздействие?		Как происходит каскадирование сбоев в работе?		Рассмотреть и количественно оценить риск.

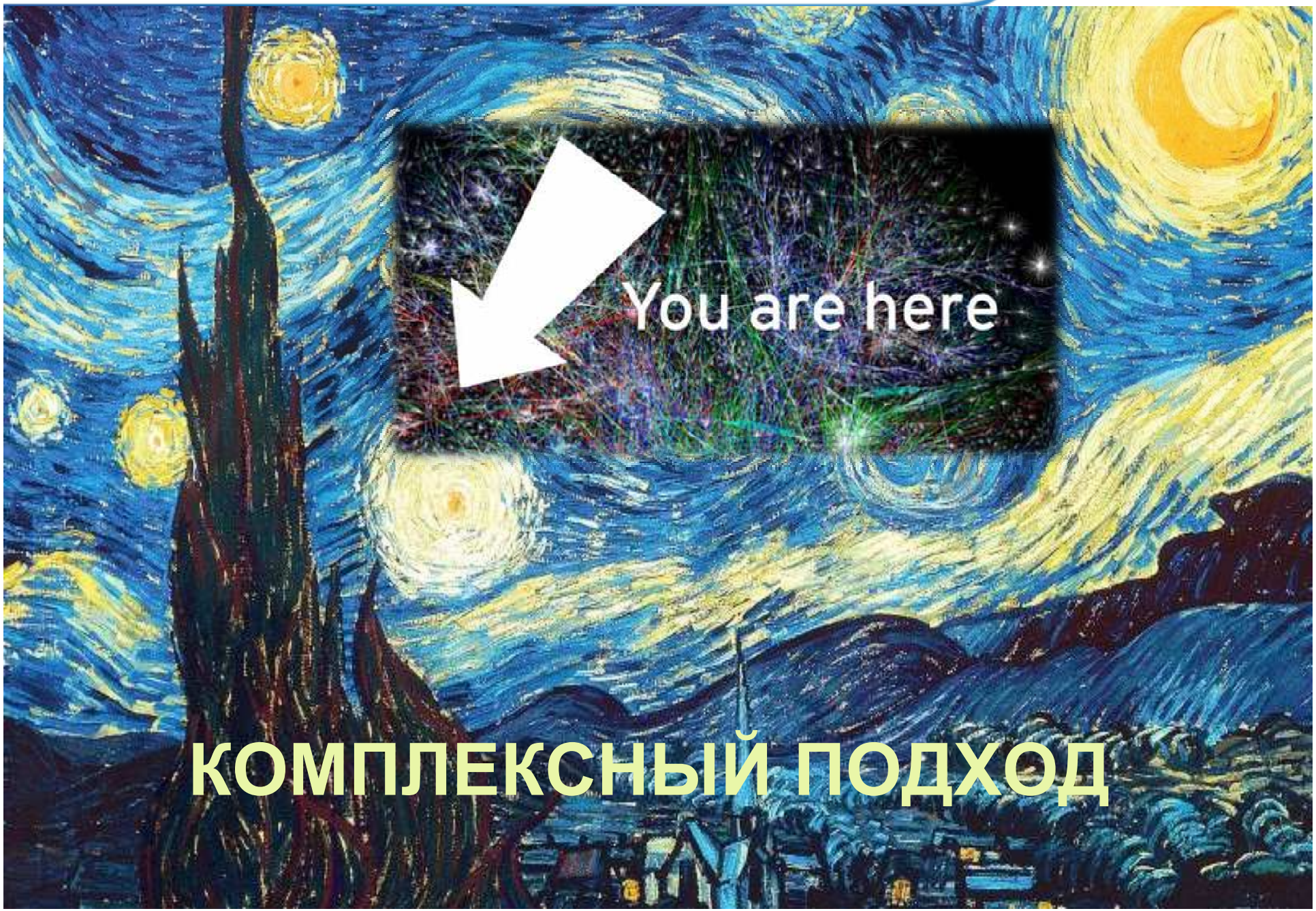
Объективные сложности

- Определение вероятности события
  - События редкие или их не было – статистика не работает
  - Даже одно событие может изменить мир, технологии и т.п.
- Расчет ущерба
  - много сценариев развития аварии с разной вероятностью
  - требуются глубокие знания технологии
  - трудно учесть взаимное влияние
- Требования регуляторов
  - не гармонизированы
  - недостаточно конкретны применительно к РЗА
  - оторваны от технологической специфики
  - не полны (не всегда актуальны текущим угрозам)
- Трудно определить Return on Investment

Стратегия оптимизации

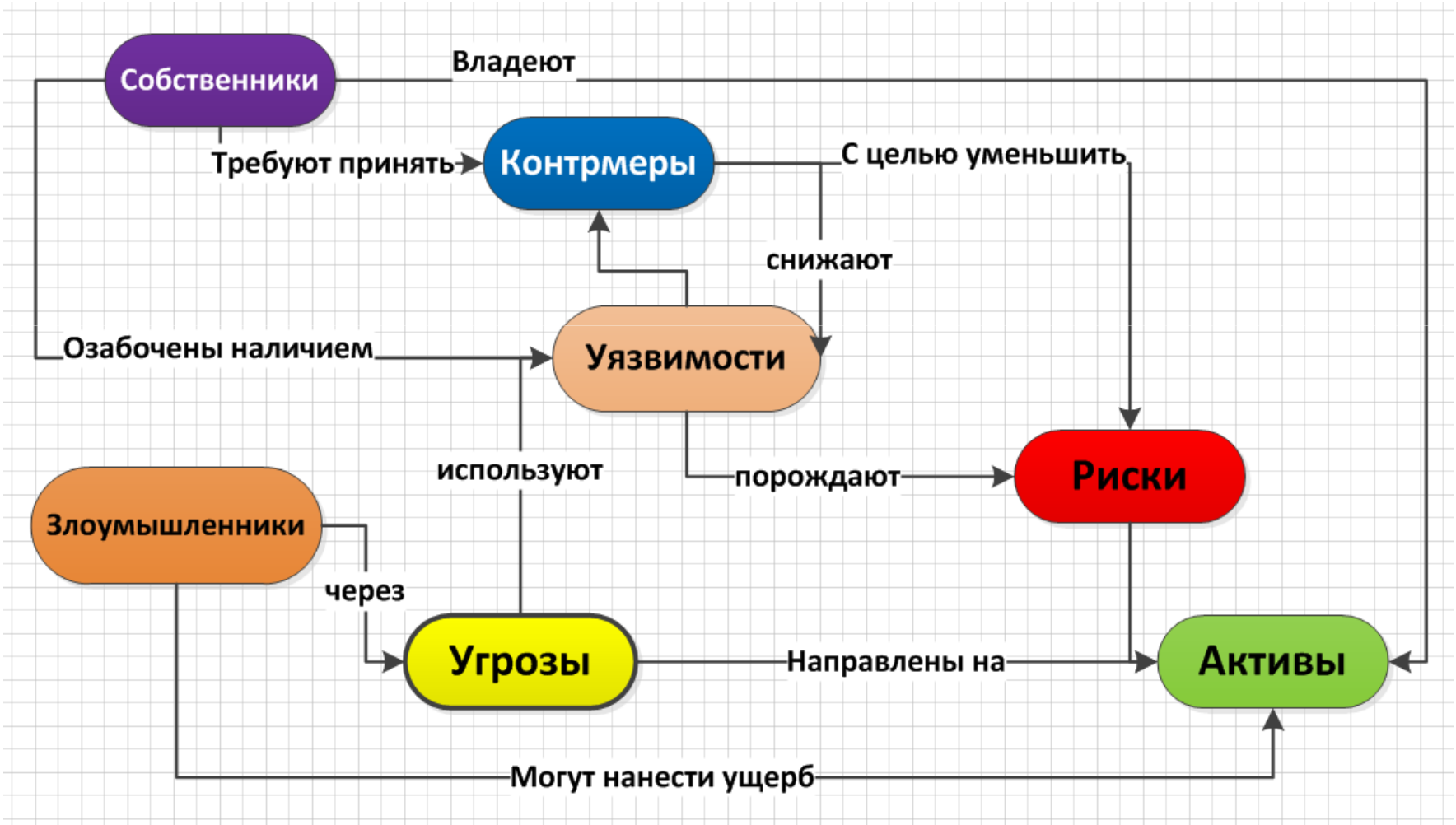
- Комплексный подход
- Упор на использование встроенных средств защиты в противовес наложенным
- «Партнёрство»
  - Налаживание взаимодействия с силовыми структурами и центрами по мониторингу угроз
  - Работа с законодателями – взлом инфраструктурных информационных систем ≠ взлому банка
- Технические решения
  - Опора на криптографию (замена шифрования хэшированием)
  - Использование новых изначально более защищенных протоколов (например, Thread для IoT), «диодов данных», DPI с фильтрацией протоколов
  - Доверенное управление (контроль ТУ, контроль прошивок и т.п.)
- Человеческий фактор
  - Введение режима «разумного» ДСП на информацию по теме
  - Изоляция подрядчиков
  - Обучение в том числе устойчивости к методам социального инжиниринга
- Научный подход: KPI, метрики и Имитационное моделирование

RTSoft

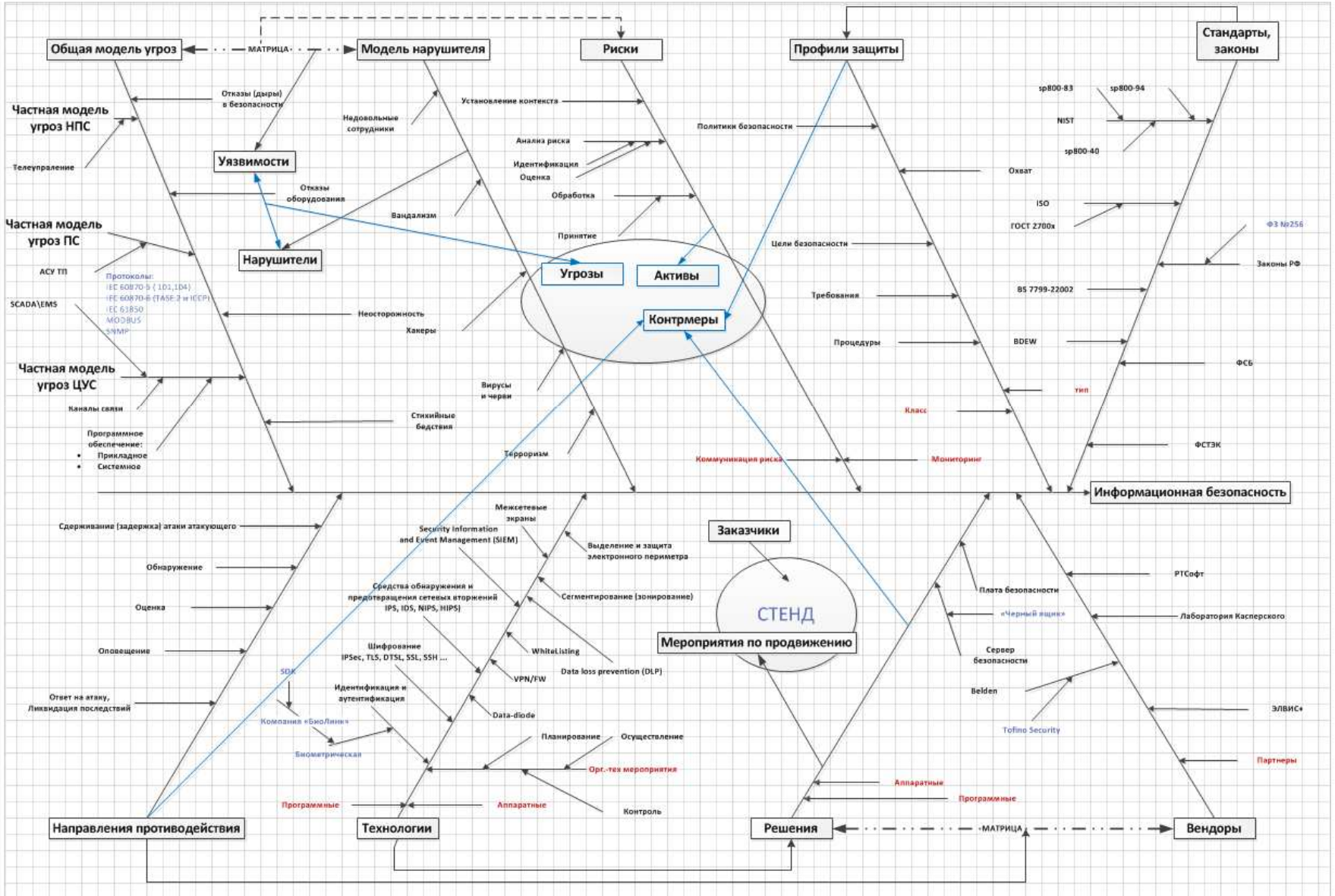


КОМПЛЕКСНЫЙ ПОДХОД

Концептуальная модель архитектуры безопасности

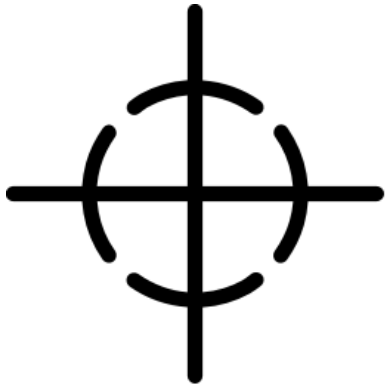


Онтологическая модель



Риски РЗА

- Выход из строя (техническая надежность)
- Ошибки настройки и программирования
  - Собственные
  - Подрядчиков
  - В ходе загрузки, настройки и программирования
- Ошибки эксплуатации
  - Недостаточный опыт и квалификация
  - Уход специалистов вместо со знаниями
- Атака злоумышленников
  - Внутренние
  - **Внешние**
  - Косвенный ущерб (например, от вирусов-шифровальщиков)



УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ

Об утверждении Доктрины информационной безопасности Российской Федерации

В целях обеспечения информационной безопасности Российской Федерации п о с т а н о в л я ю:

1. Утвердить прилагаемую Доктрину информационной безопасности Российской Федерации.

2. Признать утратившей силу Доктрину информационной безопасности Российской Федерации, утвержденную Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.

3. Настоящий Указ вступает в силу со дня его подписания.

Президент Российской Федерации * 5 * КАНЦЕЛЯРИЯ

Президент
Российской Федерации В.Путин

Москва, Кремль
5 декабря 2016 года
№ 646

Руководство к действию

27. Основными направлениями обеспечения информационной безопасности в области науки, технологий и образования являются:

а) достижение конкурентоспособности российских информационных технологий и развитие научно-технического потенциала в области обеспечения информационной безопасности;

б) создание и внедрение информационных технологий, изначально устойчивых к различным видам воздействия;

встроенные средства

в) проведение научных исследований и осуществление опытных разработок в целях создания перспективных информационных технологий и средств обеспечения информационной безопасности;

г) развитие кадрового потенциала в области обеспечения информационной безопасности и применения информационных технологий;

36. Задачами государственных органов в рамках деятельности по развитию и совершенствованию системы обеспечения информационной безопасности являются:

в) совершенствование информационно-аналитических и научно-технических аспектов функционирования системы обеспечения информационной безопасности;

В том числе **моделирование**

Хорошее основание для НИР и ОКР

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

РАСПОРЯЖЕНИЕ

от 5 декабря 2016 г. № 2589-р

МОСКВА

1. Внести в Государственную Думу Федерального Собрания Российской Федерации проекты федеральных законов "О безопасности критической информационной инфраструктуры Российской Федерации", "О внесении изменений в законодательные акты Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" и "О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации".

В пакет входят три документа:
- проект ФЗ «**О безопасности критической информационной инфраструктуры (КИИ) РФ**»,
- «О внесении изменений в законодательные акты РФ …
- «О внесении изменений в Уголовный кодекс РФ и Уголовно-процессуальный кодекс РФ…

Головной исполнитель - ФСБ России.

Соисполнители: Минкомсвязь России, МВД России, ФСО России, ФСТЭК России, Минэкономразвития России, Минпромторг России.

Управление уязвимостями

Центры реагирования на инциденты компьютерной безопасности:

- Международные
  - Computer Emergency Response Team (CERT)
  - Computer Security Incident Response Team (CSIRT)
- Российские
  - Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА)*
  - CERT Ростеха
  - ФГБУ «САЦ Минэнерго России»
  - Системный Оператор и Техническая инспекция ЕЭС
  - Прочие (GOVCERT.RU, FinCERT, CERT-GIB)
  - Лаборатория Касперского

*Указ Президента Российской Федерации от 15 января 2013 г. N 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» и «Концепцией государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» утвержденной Президентом РФ 12.12.2014 № К 1274

Матрица управления рисками

- Ценность актива
- Вероятность угрозы
- Вероятность уязвимости

* Пример визуализации в SIEM

Ценность актива	Вероятность угрозы								
	L (Низкая)			M (Средняя)			H (Высокая)		
	Вероятность уязвимости								
	L	M	H	L	M	H	L	M	H
0	0	0	0	1	1	1	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8

Перерасчет в «реальном времени».
Переход от качественных оценок к метрикам

ТЕХНИЧЕСКИЕ РЕШЕНИЯ

Концепция доверенного телеуправления

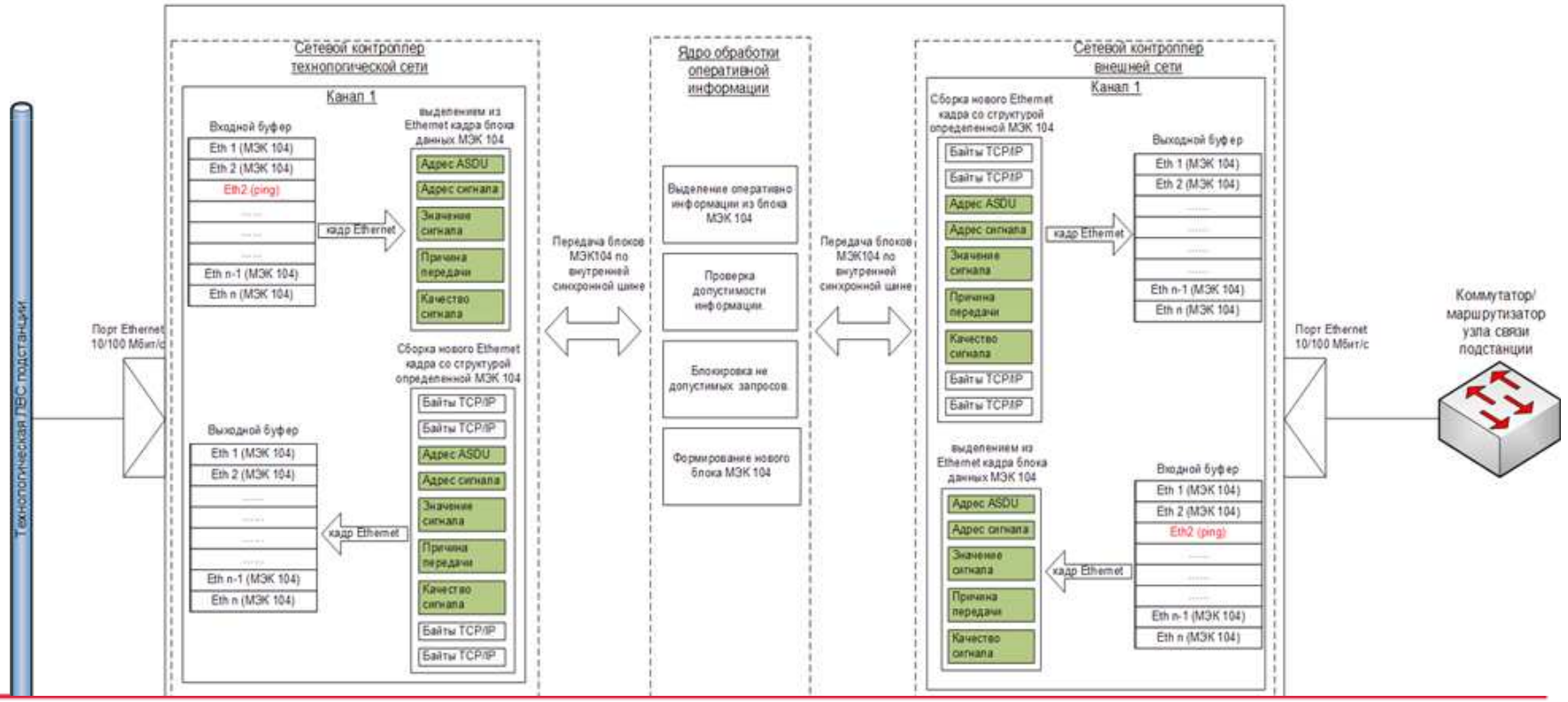
Технологическое видеонаблюдение

ИДЕЯ – технологическое видеонаблюдение позволяет получить альтернативный поток данных объекта управления. Его целесообразно использовать, когда есть основания не доверять телеметрической информации или ее поток прерван.

- Фактическое состояние оборудования механизмов и органов управления до и после выполнения операции
- Отсутствие людей вблизи исполнительных механизмов (дополнительная безопасность)
- Использование камер в инфракрасном диапазоне – температурное наблюдение
  позволяет в автоматическом режиме диагностировать, как технологические нарушение (перегрев, неравномерный нагрев и т.п.), так и появление людей

Эшелонированная оборона

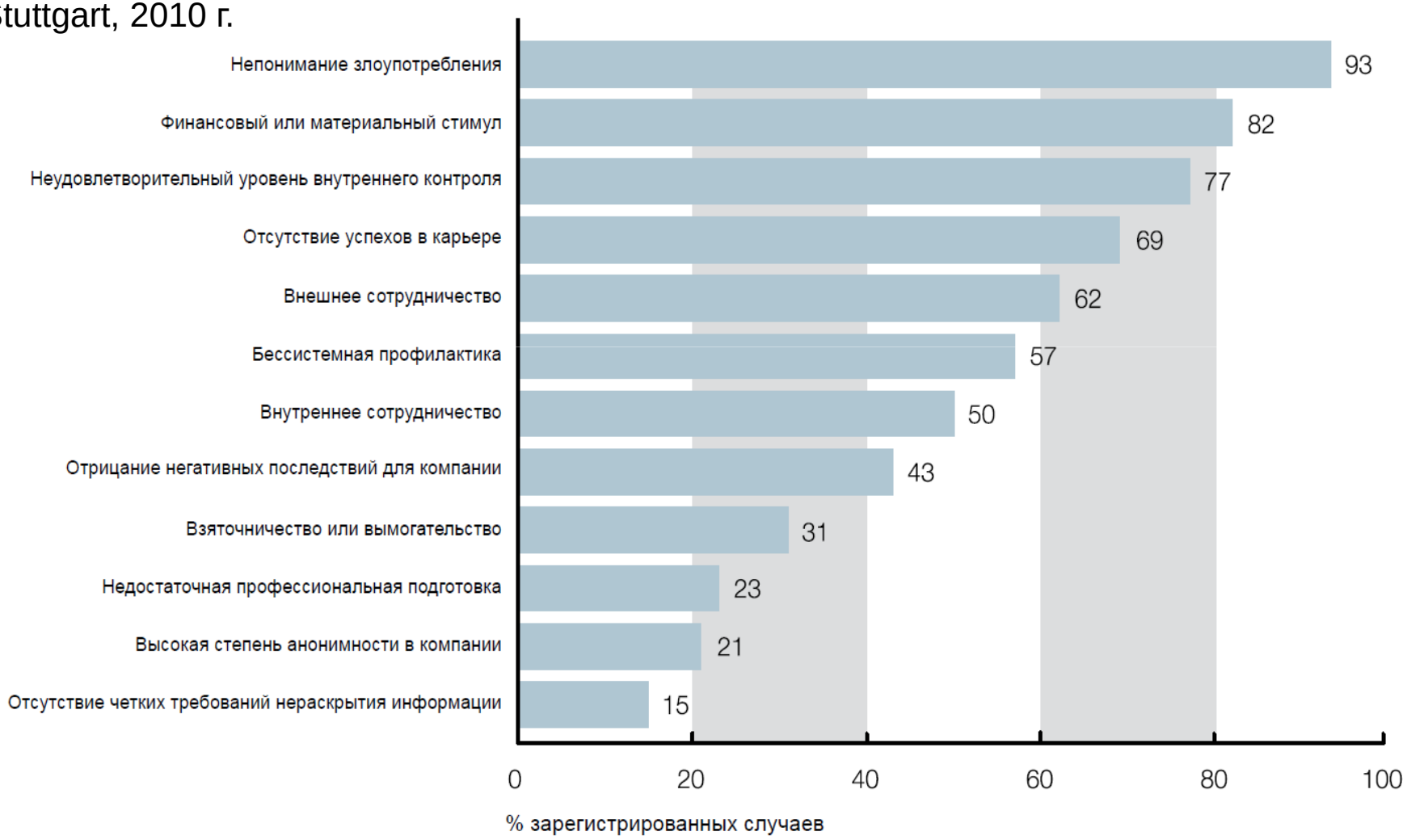
- Криптография: замена шифрования «хэшированием»
- Диоды данных
- Фильтры данных DPI с автоматической «перепаковкой»



ЧЕЛОВЕЧЕСКИЙ ФАКТОР

Мотивация внутренних нарушителей

Источник: SiFo-Studie 2009/10. Know-how-Schutz in Baden-Württemberg. Steinbeis-Edition Stuttgart, 2010 г.



Человеческий фактор

берем за основу методологию TQM и создаем
на этой основе Total Security Management (**TSM**).
Вместо «кружков качества» будут «группы безопасности» и т.п.

- Популяризация знаний ИБ, регулярное обучение – (хороший старт «игры» Лаборатории Касперского)
- Вовлеченность и стимулирование «правильного поведения» через идею TSM
- Включение собственного персонала в модель нарушителя – увы, «враг не только снаружи»
- Тройной контроль и запрет нежелательного поведения*:
  - через распорядительную документацию;
  - объективный контроль исполнения;
  - использование программно-аппаратных средств.

**Например. Запрет использования 3G модемов и Wi-Fi контролируется, а в серверных помещениях «дублируется» глушителями сигнала.*

Типизация нарушителей

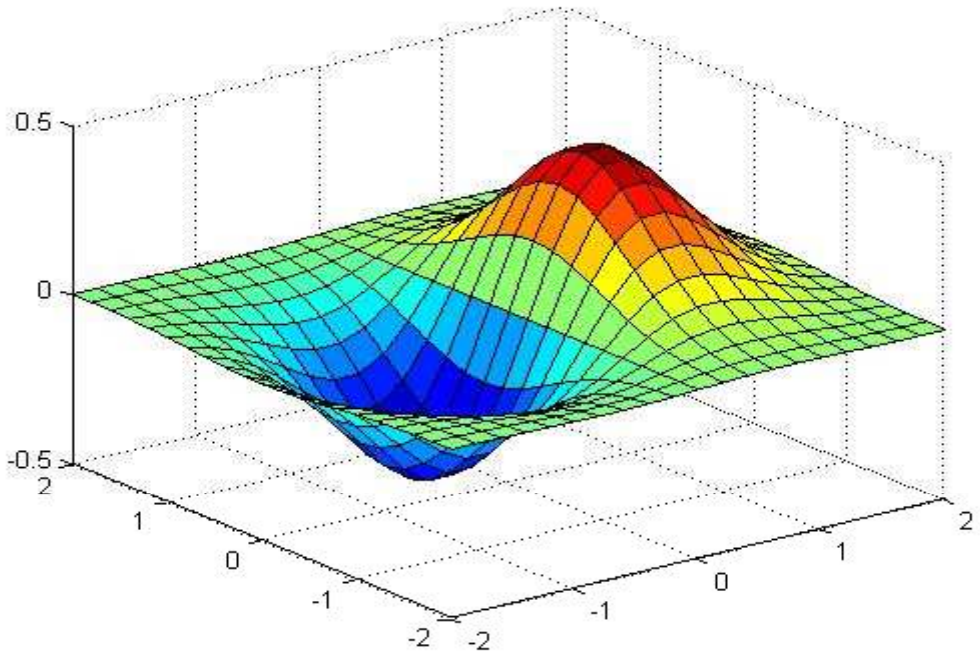
- **«Любитель»**
  - Частное лицо, пытающееся найти возможности и технологии взлома SCADA систем, имеющих интерфейсы в Интернет с помощью известных уязвимостей, найденных с использованием, например, поисковой системы «Shodan»
- **«Инсайдер»** (в том числе «без злого умысла»)
  - недовольный сотрудник или обслуживающий персонал собственной или сторонних организаций (поставщики, партнеры, наладчики), имеющий права доступа и знающий тонкости эксплуатации систем и способы хранения конфиденциальных данных
- **«Враг»**
  - Преступные группировки и иностранные правительства (Cyber Espionage, Cyber Crime, Cyber Activism, Cyber Terrorism, Cyber War и т.п.)

[Мотивация] x [Ресурс] x [Знания, опыт] x [Информированность]

Этим можно «управлять»!

Излишняя «откровенность»

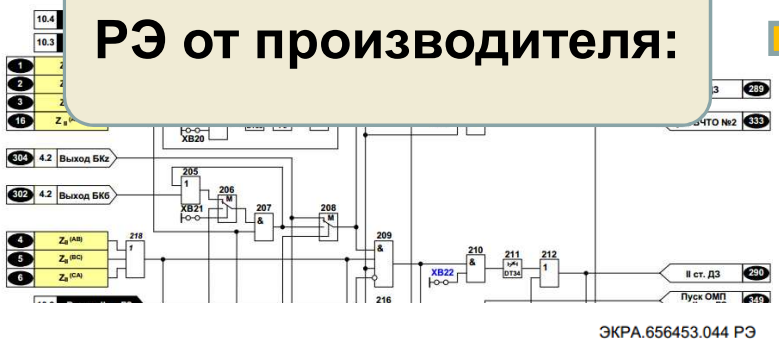
- Пример:
  - Название: «Целевые атаки на промышленные ИС»
  - Автор: Денис Легезо, Лаборатория Касперского
- Структура презентации
  - Цель: выяснить, возможно ли получить полное управление АСУТП
  - Тестовый стенд:
  - Средства для атаки:
  - • Шаг 1: сканируем nmap-ом сеть снаружи...
  - ...
  - • Шаг 12: Получаем полный контроль над тех. процессом через WinCCExplorer или WebNavigator

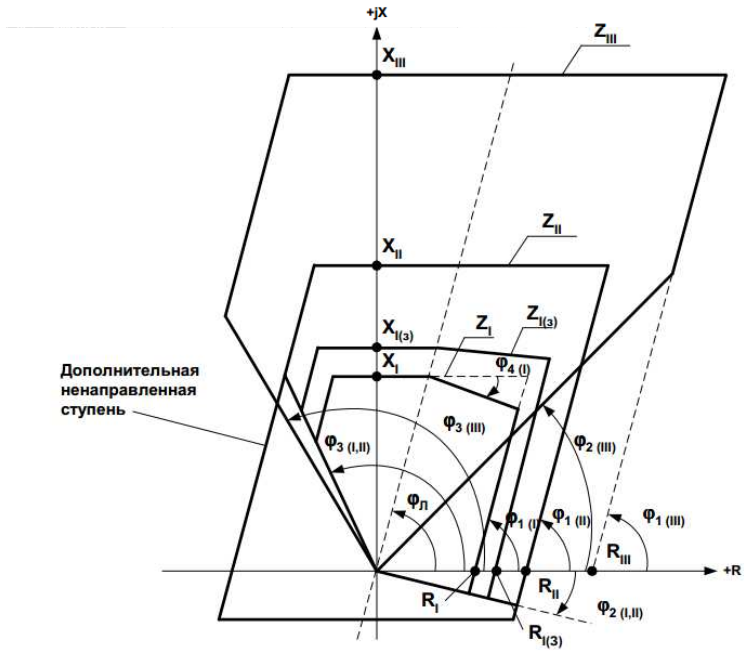


НАУЧНЫЙ ПОДХОД И ИНСТРУМЕНТЫ

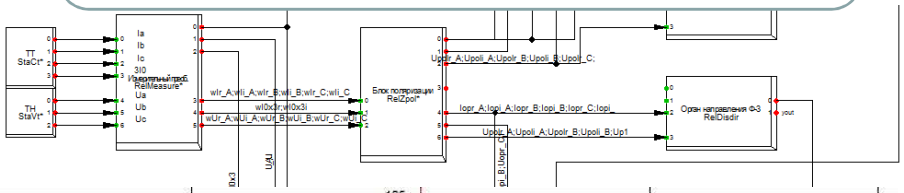
Моделирование РЗА в PF.Protection

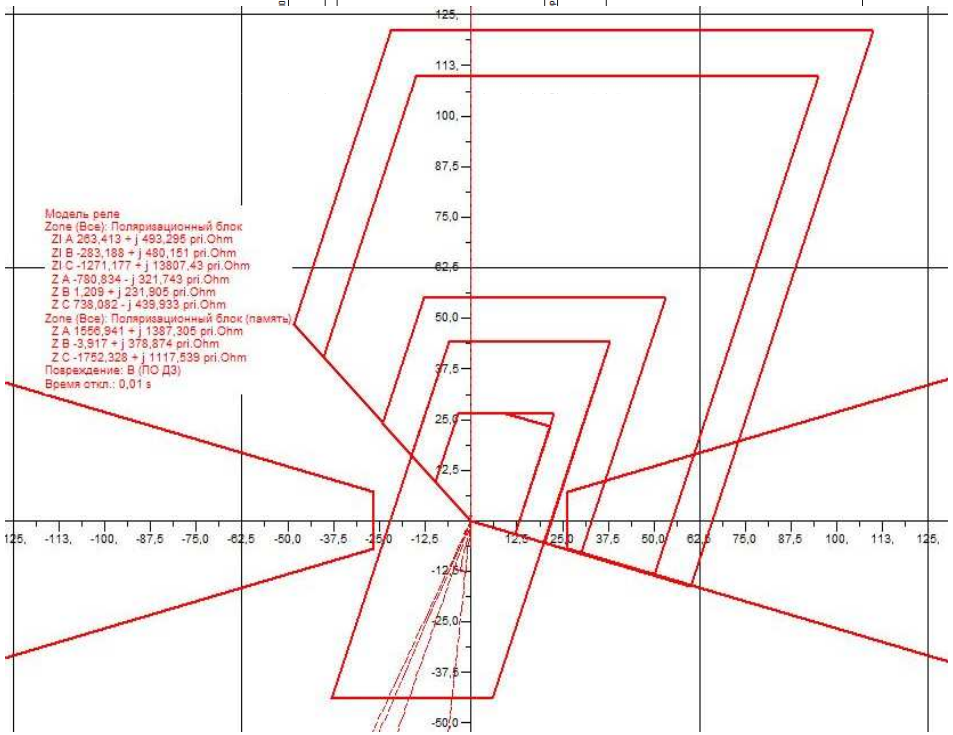
РЭ от производителя:





Модель в PF.Protection





Для оценки возможного ущерба + вероятность

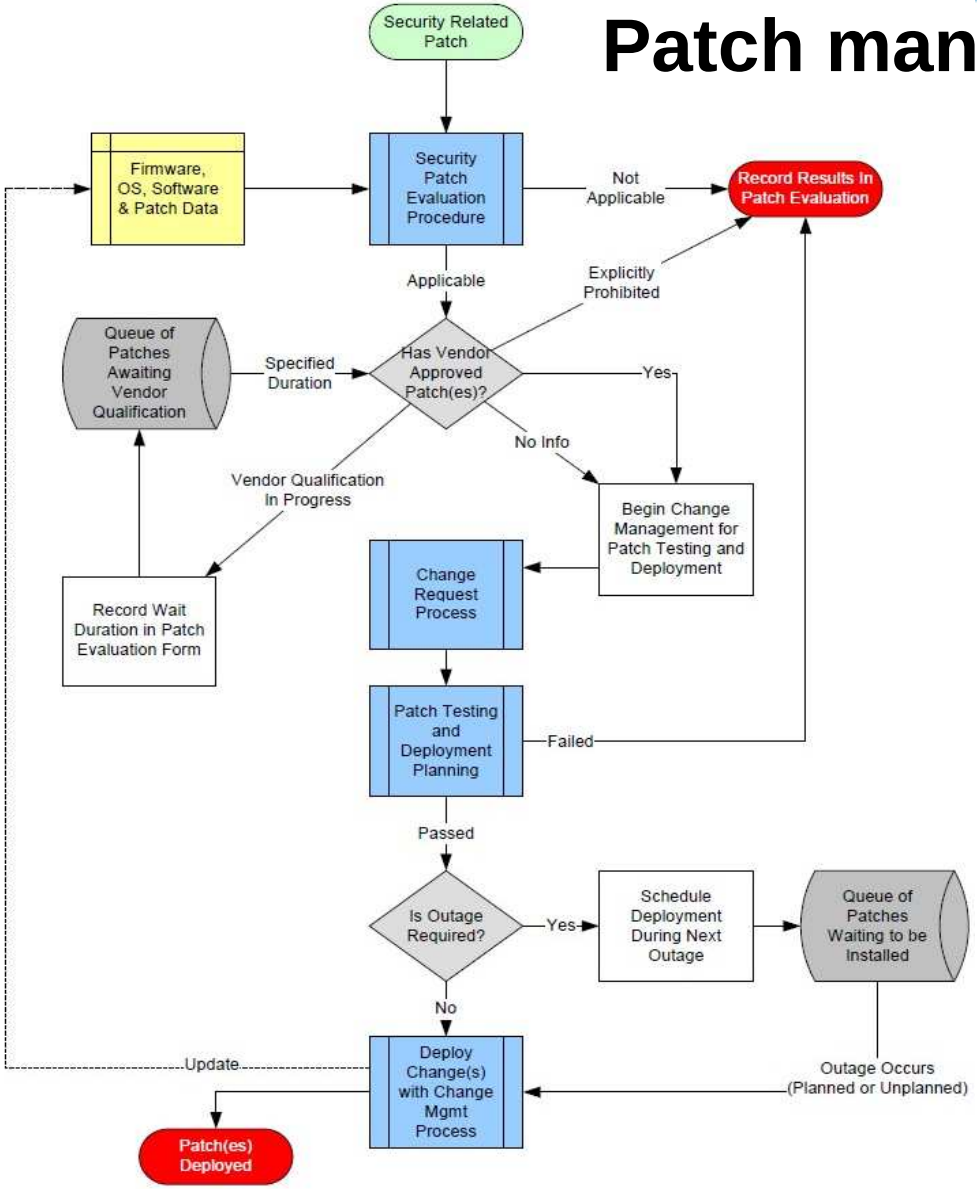
Разработанные модели РЗА

1. ЭПЗ-1636
2. ЭПЗ-1644
3. ПДЭ-2001
4. ПЗ-5
5. ДЗ-503
6. ШЭ2607 011
7. ШЭ2607 016
8. ШЭ 2607 021
9. ШЭ2607 072
10. ШЭ2710 511
11. ШДЭ-2801
12. СИРИУС-3ЛВ
13. МФТЗ
14. AREVA P437 (для РФ)

1. ABB
2. AEG
3. Alstom
4. Areva
5. GE
6. Schneider
7. Siemens
8. Sprecher

Подробнее на Конференции в 2017г и в материалах B5 CIGRE!

Patch management



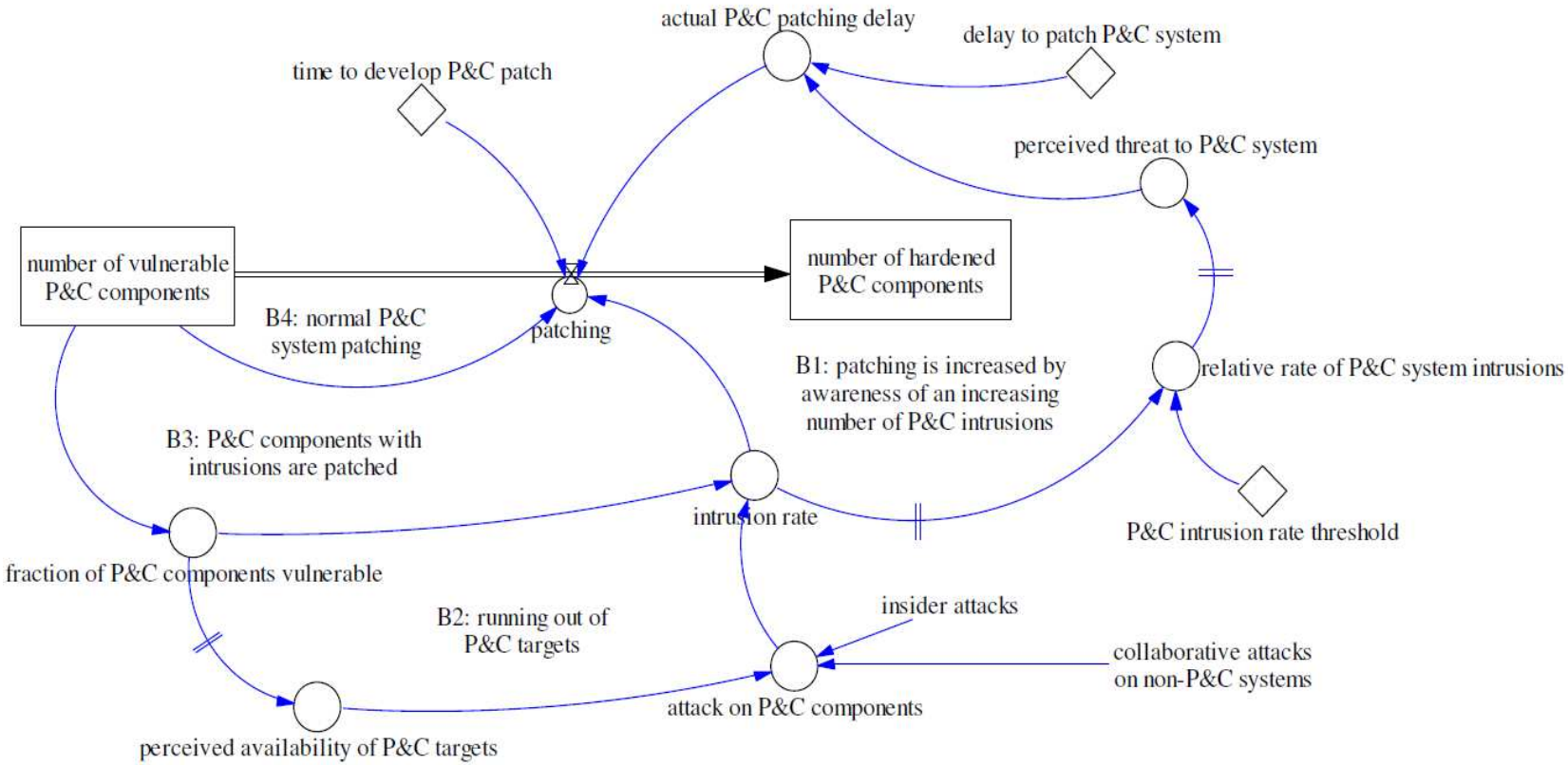
Направления оптимизации:

- ждать до следующего планового отключения для вывода в ремонт или технического обслуживания;
- инициировать немедленное обновление и мириться с потерями;
- изменить график ТОиР, если потери от простоя значительные, но нельзя откладывать обновление из-за высоких рисков

A Manual for the Cyber Security Modeling Language. **Hannes Holm, Mathias Ekstedt, Teodor Sommestad, Matus Korman**
Stockholm : Department of Industrial Information and Control Systems, Royal Institute of Technology, 2014

Моделирование

Модель системной динамики для применения исправлений ПО



*В случае большого парка оборудования и потока работ по обновлению ПО и прошивок контроллеров, оптимизация на большой промежуток времени

Источник: Application and Management of Cybersecurity Measures for Protection and Control Systems. **CIGRE, Joint Working Group B5/D2.46.** 2014.

Где находимся, куда движемся: KPI и метрики

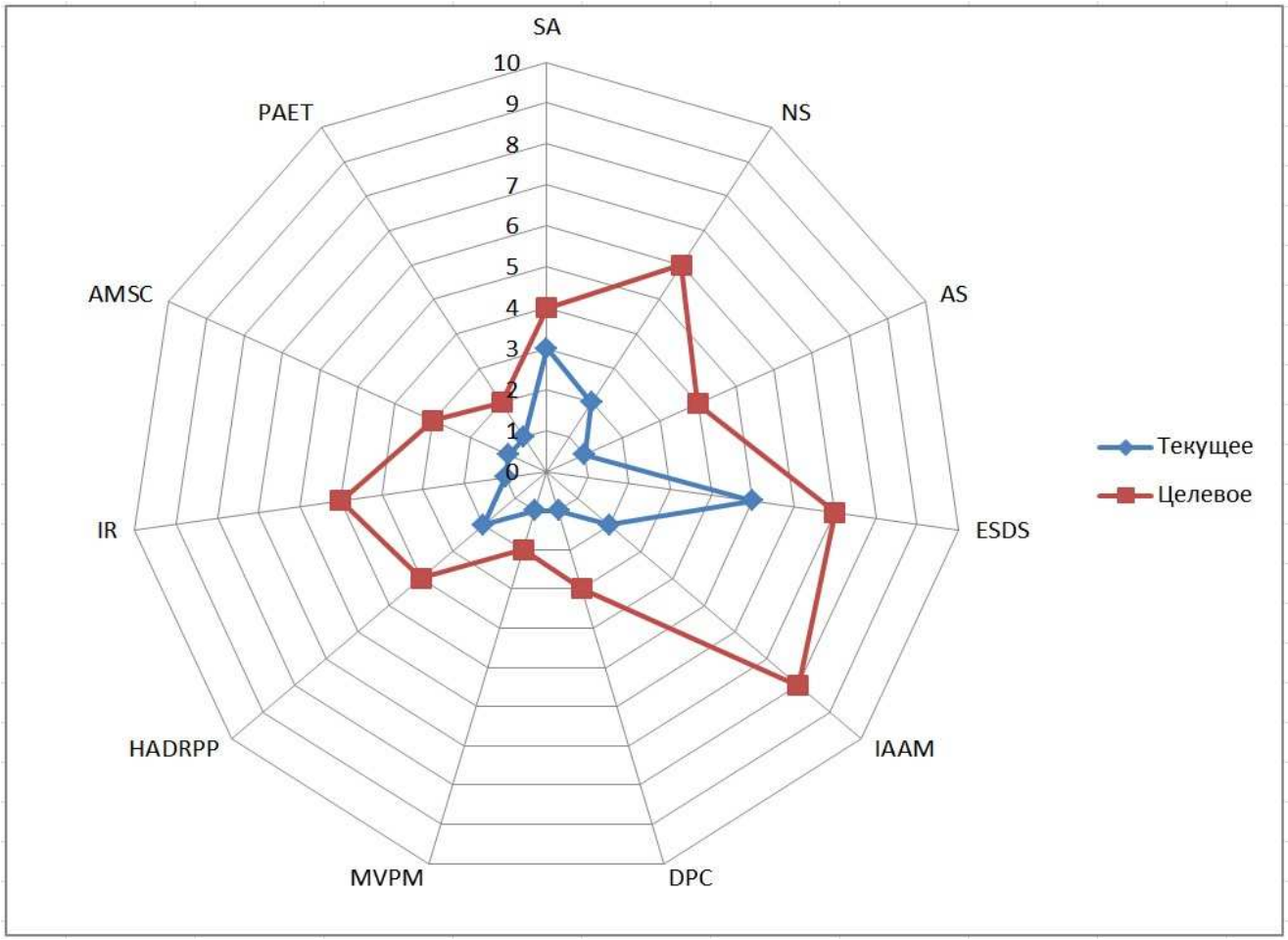
1шаг - оценка масштаба: 10; 100; 1000; 10 000 – метрика м.б. комплексной (компьютеры, люди, телекоммуникационное оборудование, ПО, серверы…)

- 2 шаг – сегментация мероприятий по обеспечению ИБ
  - Системное администрирование (SA)
  - Сетевая безопасность (NS)
  - Безопасность приложений (AS)
  - Безопасность рабочих станций, серверов и устройств (ESDS)
  - Идентификация, аутентификация и управление доступом (IAAM)
  - Защита данных и криптография (DPC)
  - Мониторинг, управление обновлениями (MVPM)
  - Аварийное восстановление и физическая защита (HADRPP)
  - Реагирование на инциденты (IR)
  - Управление активами и поставками (AMSC)
  - Политики безопасности, аудит и обучение персонала (PAET)

В каждом сегменте есть разделы и вопросы, позволяющие сделать экспертную оценку

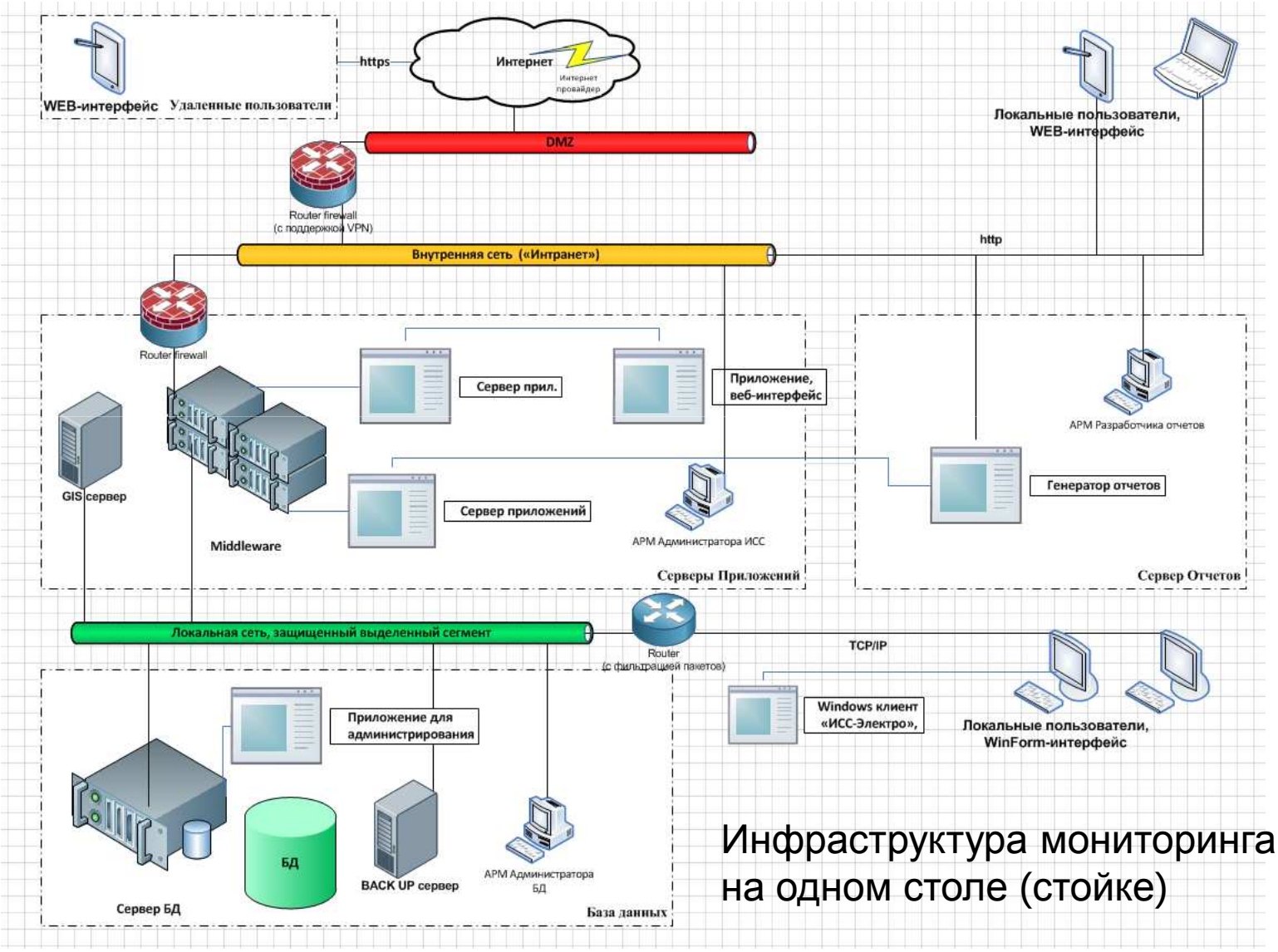
Источник: **Scott Donaldson, Stan Siegel, Chris Williams, Abdul Aslam.** *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats.* б.м. : Apress, 2015

Представление текущего и целевого состояния



В зависимости от выбранного стандарта количество доменов может колебаться от 10 до 35!

ИС поддержки жизненного цикла ИБ



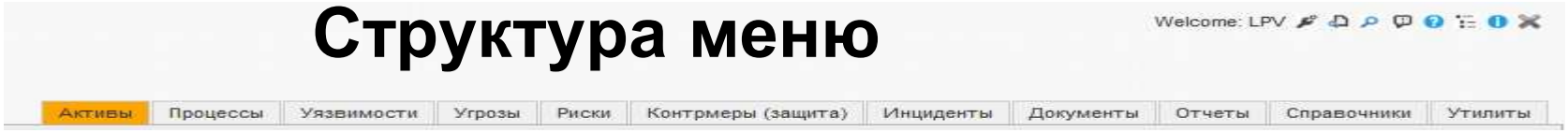
Инфраструктура мониторинга ИБ на одном столе (стойке)

ПО «Моделирования и поддержки жизненного цикла решений по обеспечению безопасности» (ISLS)

Основными целями разработки и применения ISLS являются:

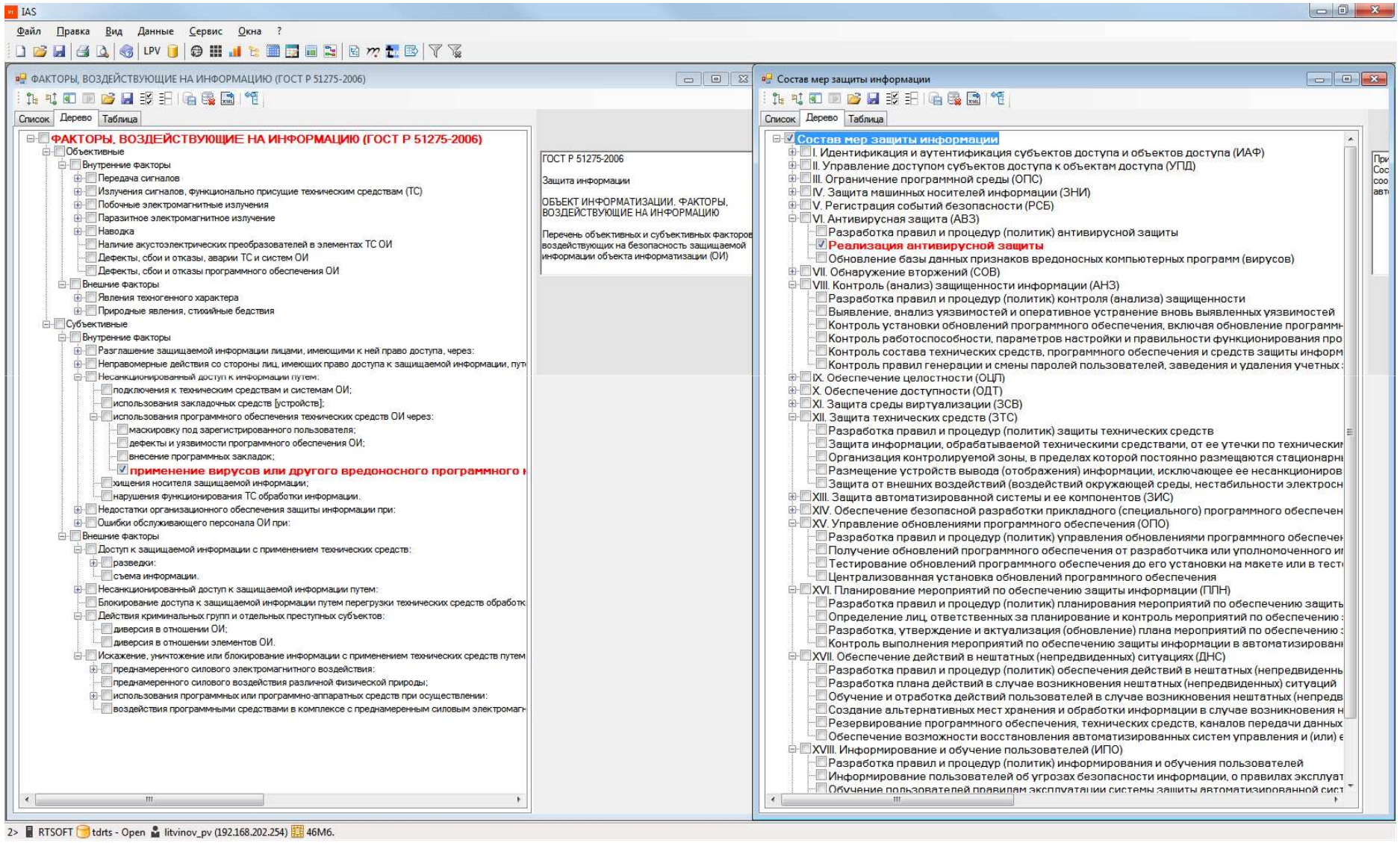
- реализация комплексного подхода к разным граням обеспечения безопасности: физической, информационной, технологической и т.д. Все составляющие необходимо развивать пропорционально, поскольку атака может быть проведена через самое слабое звено;
- системный подход к моделированию и прогнозированию. Безопасность системы, это в общем случае, сложная и нелинейная функция от состояния ее компонентов;
- определение необходимой достаточности и экономической целесообразности – оптимизация затрат на безопасность путем расчета рисков, при наличии статистических данных или моделирования рисков для новых видов угроз;
- непрерывная адаптация моделей и генерируемых на их основе документов, под меняющиеся угрозы и условия внешней и внутренней среды;
- обеспечение онтологической связности – прогнозирование через моделирование прямых и косвенных последствий событий и принимаемых решений и отдаваемых команд;
- конвергенции технологий и услуг – с целью дополнительного резервирования или исключения не рационального дублирования;
- проектирование эшелонированных мероприятий и решений по защите и активному противодействию угрозам.

Структура меню



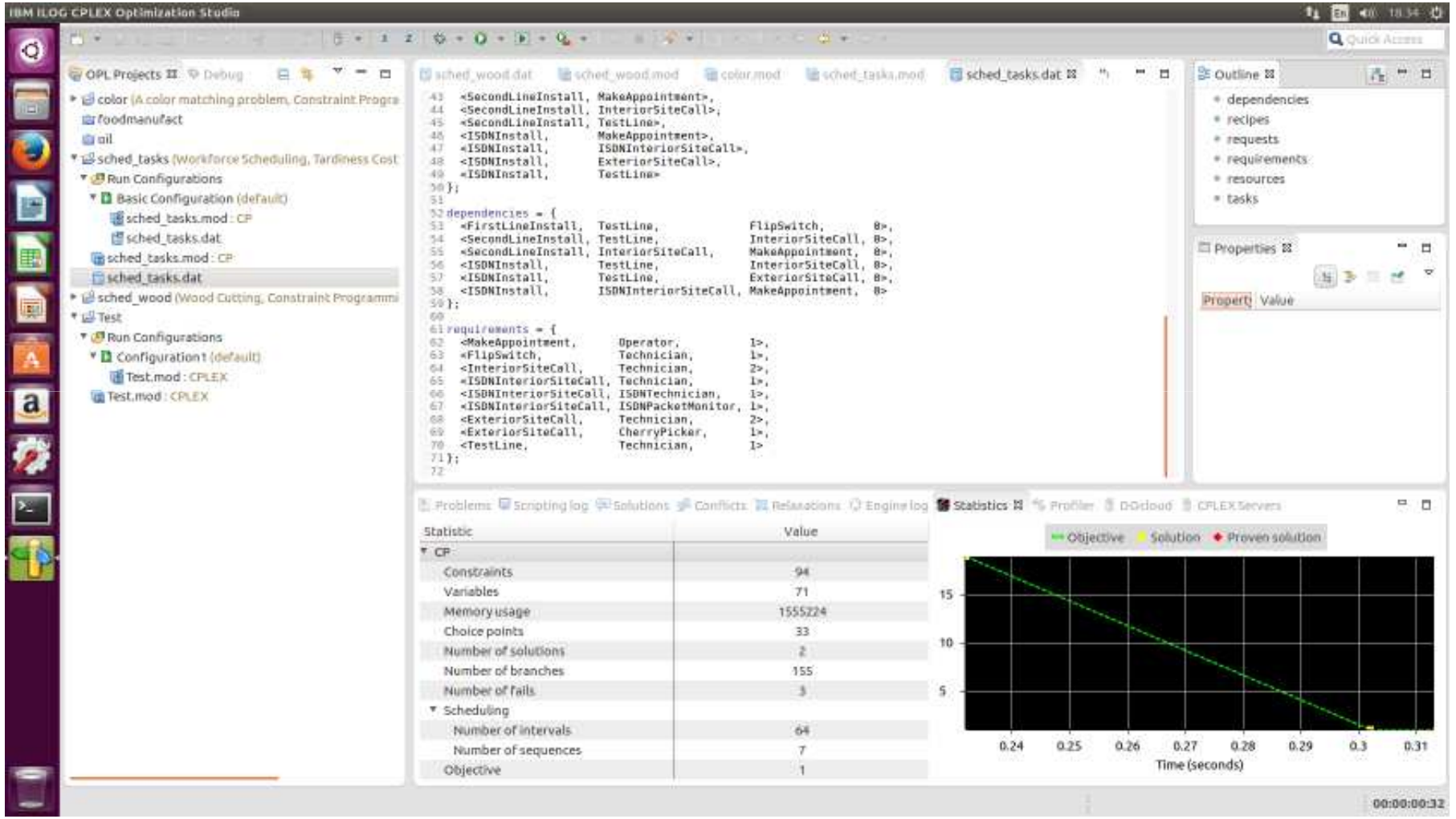
- **Активы**
  - Организационная модель
  - Объекты защиты
  - Классификатор активов
  - Реестр активов
- **Процессы**
  - Классификатор процессов
  - Бизнес-процессы
  - Технологические процессы
  - Процессы ИТ
  - Матрица ответственности
  - Процессы менеджмента ИБ
  - Процедуры ИБ
  - Аудит ИБ
- **Уязвимости**
  - Классификатор уязвимостей
  - Форма регистрации выявленной уязвимости
- **Угрозы**
  - Классификатор угроз
  - Классификатор нарушителей
  - Реестр угроз
- **Риски**
  - Классификатор рисков
  - Мониторинг рисков
  - Оценки рисков
  - Анализ рисков
  - Коммуникация рисков
- **Контрмеры (защита)**
  - Политика ИБ
  - Цели ИБ
  - Критерии ИБ
  - Объект защиты
  - Профиль защиты
  - Защитные меры
- **Инциденты**
  - Классификатор инцидентов
  - Форма регистрации инцидента
- **Документы**
  - Законы
  - Стандарты
  - Инструкции
- **Справочники**
  - Технологии защиты
  - Поставщики решений
  - Решения по защите
  - Глоссарий терминов
- **Утилиты**
  - Генератор отчетов
  - Импорт
  - Экспорт
  - События триггеры
  - Уведомления

Интерфейс для аналитики



[Факторы воздействующие на информацию (ГОСТ)] x [Меры защиты (ФСТЭК)]

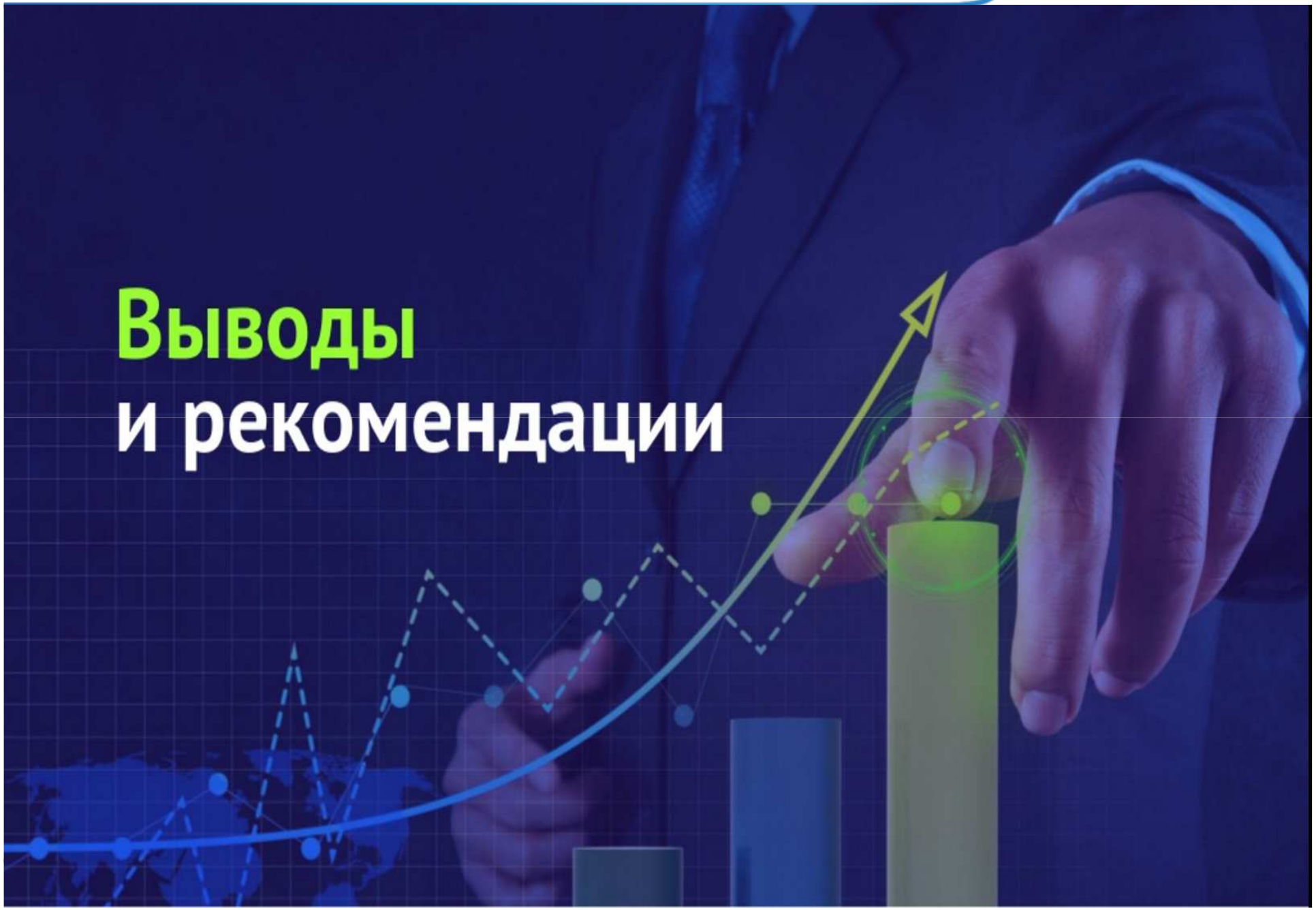
IBM ILOG CPLEX Optimization Studio



Оптимизация бизнес-решений с помощью

OPL - Optimization Programming Language

RTSoft



Стратегия оптимизации

- Комплексный подход
- Упор на использование встроенных средств защиты в противовес наложенным
- «Партнёрство»
  - Налаживание взаимодействия с силовыми структурами и центрами по мониторингу угроз
  - Работа с законодателями – взлом инфраструктурных информационных систем <> взлому банка
- Технические решения
  - Опора на криптографию (замена шифрования хэшированием)
  - Использование новых изначально более защищенных протоколов (например, Thread для IoT), диодов-данных, DPI с фильтрацией протоколов
  - Доверенное управление (контроль ТУ, контроль прошивок и т.п.)
- Человеческий фактор
  - Введение режима «разумного» ДСП на информацию по теме
  - Изоляция подрядчиков
  - Обучение в том числе устойчивости к методам социального инжиниринга
- Научный подход: KPI, метрики и Имитационное моделирование

Тактика оптимизации

- Принятие рисков
  - в модель угроз включаем только критические риски
- Принцип Парето
  - (в каждом направлении выполняем только «дешевые шаги»)
- «Чуть лучше, чем у других»
  («не надо уметь бегать быстрее, чем медведь гризли…»)
- «Не моя война»
  - Вы не можете и (не должны!) самостоятельно противостоять таким угрозам как Cyber Espionage, Cyber Crime, Cyber Activism, Cyber Terrorism, Cyber War – расставляем Honeypots/Honeynets/Honeytokens для **обоснованного** обращения за помощью
- «Чужой бюджет» (времени и денег)
  - обучение, IT – инфраструктура, модернизация … и т.п.
  - согласование с планами работ других подразделений

Вопросы?

Спасибо за внимание!

Павел Литвинов,
начальник аналитического отдела

litvinov_pv@rtsoft.ru

ЗАО «РТСофт»
тел. +7 (495) 742-68-28, 967-15-05